W1218

FIREWALL AND ITS METHOD

Patent Number: JP2000156711
Publication date: 2000-06-06
Inventor(s): AOYANAGI KOICHI
Applicant(s): NEC CORP
Requested Patent: JP2000156711
Application Number: JP19980328610 19981118
Priority Number(s):
IPC Classification: H04L12/66; H04L9/32; H04L12/28; H04L12/56
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To cope with plural programs and to prevent the entry of an unauthor ized user by storing a data-verifying method in a storage means as a program corresponding to inputted data, discriminating and verifying the inputted data by plural kinds of data discrimination and verification programs which are stored in the storage means.
SOLUTION: A program compatible with received data is called from a data-verifying method auxiliary storage part 24 to data to be inputted from an input device 1, and the contents of the received data are discriminated by the called program by a received data-discriminating means 21. Discrimination is performed according to the starting order to be created by a data verification order creating means 22. The starting order of the program to be executed by the received data discriminating means 21 for discriminating the contents of the received data and the starting order of the program to be executed by a data-verifying means 23 for discriminating the propriety of access from an external computer are created by the data verification order creating means 22. The data verifying means 23 calls programs according to the order created by the order creating means 22.

TOP

W1218

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－156711
（P2000－156711A）
(43)公開日　平成12年６月６日(2000.6.6)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ	５Ｊ１０４
9/32		9/00	６７１	５Ｋ０３０
12/28		11/00	３１０Ｚ	５Ｋ０３３
12/56		11/20	１０２Ａ	

審査請求　有　請求項の数６　ＯＬ　（全９頁）

(21)出願番号　特願平10－328610

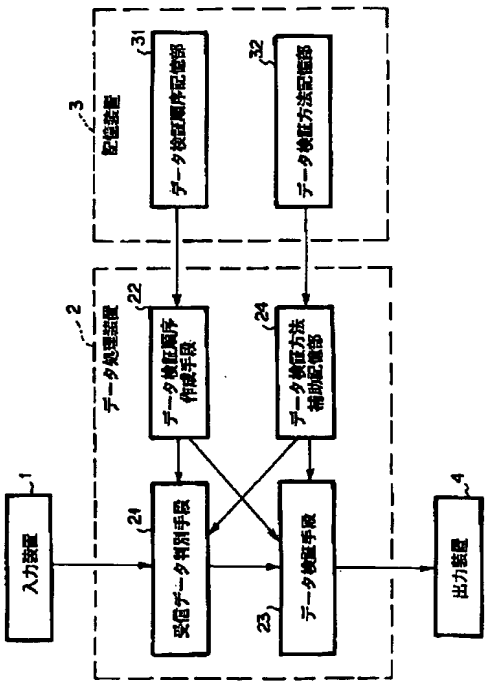
(22)出願日　平成10年11月18日(1998.11.18)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　青柳　孝一
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100065385
弁理士　山下　穣平

Ｆターム(参考)　5J104 AA07 KA01 PA07
5K030 GA07 GA15 HB19 HC01 HC14 HD03 HD06 JT02 KA01 KA04 MB18
5K033 AA08 BA04 CB08 DA06 DB12 DB14 DB20 EC04

(54)【発明の名称】　ファイアーウォールとその方法

(57)【要約】
【課題】　複数のプログラムに対処でき、外部に流通しているプログラムに応じて不正なユーザの侵入に対して防御できるファイアーウォールシステム及びその方法を提供することを課題とする。
【解決手段】　外部ネットワークから妨害データの侵入を阻止するファイアーウォールにおいて、入力データに対応してデータ検証方法をプログラムとして格納する記憶手段を備え、前記入力データを前記記憶手段に格納された複数種類のデータ判定・検証プログラムによって判定・検証することを特徴とする。



【特許請求の範囲】
【請求項１】　外部ネットワークから妨害データの侵入を阻止するファイアーウォールにおいて、
入力データに対応してデータ検証方法をプログラムとして格納する記憶手段を備え、前記入力データを前記記憶手段に格納された複数種類のデータ判定・検証プログラムによって判定・検証することを特徴とするファイアーウォール。
【請求項２】　請求項１に記載のファイアーウォールにおいて、前記入力データを入力する入力装置と、プログラムの制御により動作するデータ処理装置と、プログラムの実行順序およびアクセス制御を行う前記プログラムを記憶する前記記憶装置と、前記入力データをシステム内部に向けて送信する出力装置とからなり、前記データ処理装置は前記記憶装置から読み出したデータ検証順序プログラムの順序に従って、データ検証プログラムを実行することを特徴とするファイアーウォール。
【請求項３】　前記データ処理装置は受信データ判別手段とデータ検証手段とを備え、前記受信データ判別手段は前記データ検証順序プログラムの順序に従って、前記データ検証プログラムに則って前記入力データの正当性を判別し、前記データ検証手段は前記データ検証順序プログラムの順序に従って、前記データ検証プログラムに則って前記入力データによってアクセスの可否を検証することを特徴とする請求項２に記載のファイアーウォール。
【請求項４】　請求項１又は２に記載のファイアーウォールにおいて、前記判定・検証することは、前記入力データのポート番号について受信データ判別手段で前記記憶手段からのポート番号判別プログラムによって判別し、次に受信データ検証手段は前記記憶手段からのポート番号検証プログラムによって検証し、次に前記入力データの接続先について受信データ判別手段で前記記憶手段からの接続先判別プログラムによって判別し、次に受信データ検証手段は前記記憶手段からの接続先検証プログラムによって検証することを特徴とするファイアーウォール。
【請求項５】　請求項１又は２に記載のファイアーウォールにおいて、前記記憶手段に格納された複数種類のデータ判定・検証プログラムは前記入力データに対応して、前記データ判定・検証プログラムを随時追加・更新し、検証順序を追加するのみで新たなデータ検証方法が実行されることを特徴とするファイアーウォール。
【請求項６】　入力データを入力する入力装置と、プログラムの制御により動作するデータ処理装置と、プログラムの実行順序およびアクセス制御を行う前記プログラムを記憶する記憶装置と、前記入力データをシステム内部に向けて送信する出力装置とからなるファイアーウォール方法において、
前記入力データのポート番号について受信データ判別手段で前記記憶手段からのポート番号判別プログラムによって判別し、次に受信データ検証手段は前記記憶手段からのポート番号検証プログラムによって検証し、次に前記入力データの接続先について受信データ判別手段で前記記憶手段からの接続先判別プログラムによって判別し、次に受信データ検証手段は前記記憶手段からの接続先検証プログラムによって検証することを特徴とするファイアーウォール方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、外部ネットワークから妨害データの侵入を阻止する装置であるファイアーウォールと、その妨害データの侵入を阻止するファイアーウォール方法に関する。
【０００２】
【従来の技術】近年、急速に普及してきているインターネットは、その標準プロトコルとしてＴＣＰ／ＩＰを採用しており、ＴＣＰ／ＩＰに従った通信をＡＴＭネットワークでも採用されており、インターネットは全世界を相手にネットワーク網を確立しようとしている。
【０００３】このインターネットの普及に伴い、コンピュータ等の端末やＬＡＮ（Local Area Network）やＷＡＮ（Wide Area Network）のサーバ等を公衆網に接続する機会が増加し、このような状況で公衆網側から不正なアクセスから端末やサーバを守る技術が重要である。この場合、特定種類のトラフィックを遮断する機能が必要になり、この特定種類のトラフィックを遮断することによって端末やサーバのセキュリティを向上させる装置をファイアーウォールと呼んでいる。
【０００４】このファイアーウォールに関して、特開平１０－２１５２４８号公報において、ＩＰ over ＡＴＭ又はLANエミュレーションを有効化するために、端末Ａが端末Ｂに対して発呼要求メッセージを出力し、このメッセージはＴＣＰ／ＩＰプロトコルによるサービスの要求を行い、端末Ａと端末Ｂ間の交換ノードの呼管理制御部で、このメッセージをエージェントに渡し、エージェントは受信した発呼要求メッセージに設定されているＩＰアドレス及びＴＣＰのポート番号がファイアーウォールテーブルに登録されているか否かを調べ、登録されていれば、端末Ｂへのアクセス要求を許容し、端末Ａと端末Ｂとの間のＡＴＭコネクションを確立し、そのＡＴＭコネクション上にＴＣＰ／ＩＰコネクションを確立し、登録されていなければ、端末Ｂへのアクセスを認めず、端末Ａと端末Ｂとの間にＡＴＭコネクションを確立せず、データの伝送を不可とすることが記載されている。
【０００５】上記公報のファイアーウォール方式では、着信先端末と着信先端末を収納する交換ノードとの間にＡＴＭコネクションを確立する必要がないので、ネットワーク資源の無駄使いを防ぎ、ＡＴＭコネクションを確立することなくアクセスが許容されるか否かが判断され

るので、その判断のために課金が発生せず、不要な課金を防止することができるとしている。

【0006】また、特開平10-154118号公報によれば、計算機間の通信に複数のファイアーウォールが介在するネットワーク通信システムに関し、計算機間の接続の管理方法について、正当なユーザが通信経路を意識することなく容易に実施できることを目的としている。

【0007】本公報では、クライアントからサーバの接続を制限する複数のファイアーウォールを有するネットワークに、ディレクトリサービスサーバを設置し、ディレクトリサービスサーバは、ネットワーク内の各計算機の識別情報、アクセス可能なユーザ、通信経路などの情報を記憶し、アクセスしてきたクライアントのユーザがサーバの正当なユーザの場合、指定されたサーバの識別情報からサーバへの通信経路の情報を検索し、中継サーバに通信経路の情報を提供し、通信経路の情報を基に中継サーバはクライアントとサーバ間の通信経路を確立する。また、ディレクトリサービスサーバとファイアーウォールとは自計算機の設定情報を互いに通信し、他の計算機でなされた設定情報の登録・更新に応じて自計算機の設定情報の登録・更新を行うとしている。

【0008】また、特開平9-270788号公報には、新しいサービスに対してもファイアーウォールをアップグレードする必要がなく、各メッセージがその送信者や宛先を確実に識別するようにすることを目的とし、データパケットに代え、そのコード自身が実行可能なコードの断片であるパケット・オブジェクトを用い、パケット・オブジェクトには、資源、宛先、主方法、方法、及びデータに対する署名からなるオブジェクト、オブジェクト・データ、及び対応オブジェクト・ヘッダが組み込まれ、資源、宛先、主方法は、クライアント・コンピュータやファイアーウォール・コンピュータの仮想マシンで実行可能コードであり、資源と宛先はパケット・オブジェクトの資源と宛先を検証するためにファイアーウォール・コンピュータにより実行され、主方法は特定の機能の提供のためサーバ・コンピュータにより実行される。

【0009】また、特開平9-252323号公報には、仮想インターネット・プロトコルに基づいた通信において、自組織に属する移動ホストだけが外部から自組織内にアクセスすることができるように、ファイアーウォールは鍵情報と移動ホストからのパケットのヘッダ情報から演算した認証情報と、パケットのヘッダ情報に含まれる認証情報とが一致する場合に、そのパケットを中継することとしている。

【0010】

【発明が解決しようとする課題】上述した各公報においては、各ファイアーウォールでは、コンピュータで受信したデータのヘッダ情報の、ポート番号や、送信元アドレスを元に、アクセスの制御を行うものであった。

【0011】しかしながら、これらの従来技術には、次のような問題点があった。

（1）従来のファイアーウォールでは、ポート番号によって通信に使用されるプログラムが決まっていることを前提として作成されており、使用するポート番号が決まっていないプログラムのことを全く考慮していないので、ポート番号が不定な場合に接続が出来ない。

（2）通常、通信データの形式は、通信を行うプログラム毎に定義されており、このデータ形式を解読できるプログラムでないと内容の確認をすることができない。従って、従来のファイアーウォールでは、ごく一部のデータ形式しか解読できないので、内容までチェックすることができなかったので、受信したデータの内容を基に、接続の可否を制御することが出来ない。

（3）従来のファイアーウォールは、製品として提供されている以外の制御方法を、利用者が追加することを何ら考慮されていなかったので、拡張のためのしくみが組み込まれていないため　従来のファイアーウォールでは、製品で定義されたアクセス制御方法しか選択出来ない。

【0012】本発明は、上記問題点を解決するため、複数のプログラムに対処でき、外部に流通しているプログラムに応じて不正なユーザの侵入に対して防御できるファイアーウォール及びその方法を提供するものである。

【0013】

【課題を解決するための手段】本発明は、外部ネットワークから妨害データの侵入を阻止するファイアーウォールにおいて、入力データに対応してデータ検証方法をプログラムとして格納する記憶手段を備え、前記入力データを前記記憶手段に格納された複数種類のデータ判定・検証プログラムによって判定・検証することを特徴とする。

【0014】また、上記ファイアーウォールにおいて、前記入力データを入力する入力装置と、プログラムの制御により動作するデータ処理装置と、プログラムの実行順序およびアクセス制御を行う前記プログラムを記憶する前記記憶装置と、前記入力データをシステム内部に向けて送信する出力装置とからなり、前記データ処理装置は前記記憶装置から読み出したデータ検証順序プログラムの順序に従って、データ検証プログラムを実行することを特徴とする。

【0015】また、上記ファイアーウォールにおいて、前記データ処理装置は受信データ判別手段とデータ検証手段とを備え、前記受信データ判別手段は前記データ検証順序プログラムの順序に従って、前記データ検証プログラムに則って前記入力データの正当性を判別し、前記データ検証手段は前記データ検証順序プログラムの順序に従って、前記データ検証プログラムに則って前記入力データによってアクセスの可否を検証することを特徴と

する。

【００１６】また、上記ファイアーウォールにおいて、前記判定・検証することは、前記入力データのポート番号について受信データ判別手段で前記記憶手段からのポート番号判別プログラムによって判別し、次に受信データ検証手段は前記記憶手段からのポート番号検証プログラムによって検証し、次に前記入力データの接続先について受信データ判別手段で前記記憶手段からの接続先判別プログラムによって判別し、次に受信データ検証手段は前記記憶手段からの接続先検証プログラムによって検証することを特徴とする。

【００１７】また、本発明は、入力データを入力する入力装置と、プログラムの制御により動作するデータ処理装置と、プログラムの実行順序およびアクセス制御を行う前記プログラムを記憶する記憶装置と、前記入力データをシステム内部に向けて送信する出力装置とからなるファイアーウォール方法において、前記入力データのポート番号について受信データ判別手段で前記記憶手段からのポート番号判別プログラムによって判別し、次に受信データ検証手段は前記記憶手段からのポート番号検証プログラムによって検証し、次に前記入力データの接続先について受信データ判別手段で前記記憶手段からの接続先判別プログラムによって判別し、次に受信データ検証手段は前記記憶手段からの接続先検証プログラムによって検証することを特徴とする。

【００１８】また、本発明は、コンピュータネットワークにおいて、利用者が外部からのアクセス制御（＝ファイアーウォール）を拡張可能とすることにより、ネットワークコンピューティングにおける、柔軟なセキュリティを提供するものである。

【００１９】また、本発明は、図１を参照して説明と、まず、入力装置１は、外部のネットワークからデータを受信する。受信データ判別手段２１は、データが受信された時に起動され、受信データの内容を判別する。判別方法は、データ検証順序作成手段２２で作成された実行順序に従って行う。

【００２０】データ検証順序作成手段２２は、データ検証順序記憶部３１から、受信データ判別手段２１で実行するプログラムの起動順序、およびデータ検証手段２３で実行するプログラムの起動順序を読み込み、それぞれの実行順序を作成する。

【００２１】データ検証手段２３は、データ検証順序作成手段２２で作成された実行順序にてプログラムを実行し、外部コンピュータからのアクセスの可否を判別する。

【００２２】データ検証方法補助記憶部２４は、データ検証方法記憶部３２から一度呼び出したデータ検証方法を格納する場所である。

【００２３】一度呼び出されたプログラムは、データ処理装置２のデータ検証方法補助記憶部２４に格納され、同じプログラムが再び必要になった時には、データ検証方法記憶部３２を参照せずに、メモリを参照することで、実行の高速化を図ることが出来る。

【００２４】データ検証順序記憶部３１は、受信データ判別手段２１で実行するプログラムの起動順序と、データ検証手段２３で実行するプログラムの起動順序を記憶している。

【００２５】データ検証方法記憶部３２は、受信データ判別手段２１で実行する受信データ判別プログラムと、データ検証手段２３で実行するアクセス制御判別プログラムを記憶している。

【００２６】尚、データ検証順序記憶部３１は、利用者により定義されたプログラム起動順序を格納することが出来、且つ、データ検証方法記憶部３２は、利用者により作成されたプログラムを格納することが出来る。

【００２７】これにより、利用者がシステムの制限にとらわれることなく、柔軟で高度なアクセス制御を行うことを可能とする。

【００２８】

【発明の実施の形態】本発明による実施形態について、図面を参照しつつ詳細に説明する。

【００２９】［本実施形態の構成］図１を参照すると、本実施形態によるファイアーウォールは、データを外部から受信する入力装置１と、プログラム制御により動作するデータ処理装置２と、プログラムの実行順序およびアクセス制御を行うプログラムを記憶する記憶装置３と、データを内部に向けて送信する出力装置４とを含む。

【００３０】入力装置１は、外部の公衆回線や専用線、ＩＳＤＮ（Integrated Service Digital Network）回線又は無線回線等のネットワークからデータを受信する。そこで、モデムやターミナル・アダプタ、ＤＳＵ（Digital Service Unit）、ルータ等が設置される。

【００３１】データ処理装置２は、受信データ判別手段２１と、データ検証順序作成手段２２と、データ検証手段２３と、データ検証方法補助記憶部２４とを備えている。

【００３２】受信データ判別手段２１は、入力装置１から入力されたデータに対して、データ検証方法補助記憶部２４からその受信データに適合するプログラムを呼び出し、呼び出されたプログラムによって受信データの内容を判別する。判別は、データ検証順序作成手段２２で作成された起動順序に従って行う。

【００３３】データ検証順序作成手段２２は、受信データの内容を判別するための受信データ判別手段２１で実行するプログラムの起動順序、および外部コンピュータからのアクセス可否を判別するためのデータ検証手段２３で実行するプログラムの起動順序を作成する。

【００３４】データ検証手段２３は、データ検証順序作成手段２２で作成された起動順序によって、データ検証

方法補助記憶部２４から該当プログラムを呼び出し、外部コンピュータからのアクセスの可否をその該当プログラムに従って判別する。

【００３５】データ検証方法補助記憶部２４は、データ検証方法記憶部３２から呼び出したデータ検証方法を格納する場所で、ＤＲＡＭやキャッシュメモリ、フラッシュメモリ等で構成される。

【００３６】記憶装置３は、データ検証順序記憶部３１と、データ検証方法記憶部３２とを備えている。例えば、ハードディスクやフロッピー（登録商標）ディスク、ＭＯ（Magneto-Optics）、ＧＩＧＡＭＯ（ギガ-Magneto-Optics）、ＣＤ－ＲＯＭ、ＤＶＤ等で構成される。

【００３７】データ検証順序記憶部３１は、受信データの内容を判別するプログラムの起動順序と、外部コンピュータからのアクセスの可否を判別するプログラムの起動順序が記憶されている。この起動順序は利用者によって定義可能である。

【００３８】データ検証方法記憶部３２は、受信データ判別プログラムと、アクセス制御判別プログラムを記憶している。このプログラムは利用者によって不図示の入力手段によって作成可能であり、又は市販の判定・検証用のプログラムをインストールしてもよい。また、このデータ検証順序記憶部３１とデータ検証方法記憶部３２とは同一記録媒体で記憶領域を区別しておいても、別個の記憶媒体で構成していてもよい。

【００３９】出力装置４は、内部のＬＡＮやＷＡＮ等のネットワークや、自身のコンピュータシステム等へ、判定・検証した結果透過してもよいデータであれば、そのまま送信する。

【００４０】［本実施形態の動作の説明］次に、図１および図２を参照して、本実施形態によるファイアーウォールシステムの動作について詳細に説明する。

【００４１】システムの起動時に、データ検証順序作成手段２２へデータ検証順序記憶部３１からデータ検証順序を格納する（ステップＡ）。

【００４２】データ検証順序作成手段２２は、データ検証のために呼び出されるプログラムの起動順序（以下、プログラム順序）を受信データ判別手段２１、およびデータ検証手段２３へ格納する（ステップＡ）。

【００４３】入力装置１よりデータを受信すると、受信データ判別手段２１にデータが供給される（ステップＢ）。

【００４４】受信データ判別手段２１は、プログラム順序内でデータ判別プログラムが格納されている場合には、プログラム順序に従い、データ検証方法補助記憶部２４に格納されたデータ判別プログラムを実行する（ステップＣ１、Ｃ３）。

【００４５】プログラム順序内でデータ判別プログラムが格納されていない場合には、データ検証方法記憶部３２から該当プログラムをデータ検証方法補助記憶部２４へ読み込み、プログラム順序に従い、データ検証方法補助記憶部２４に格納されたデータ判別プログラムを実行する（ステップＣ２、Ｃ３）。

【００４６】但し、受信データ判別手段２１が始めて呼び出される場合には、データ検証方法補助記憶部２４には受信データ判別プログラムは格納されていない。この場合には前述同様、データ検証方法記憶部３２から該当プログラムをデータ検証方法補助記憶部２４へ読み込み、プログラム順序に従い、データ検証方法補助記憶部２４に格納されたデータ判別プログラムを実行する（ステップＣ２、Ｃ３）。

【００４７】尚、ここで実行されるプログラムは、予め標準製品として提供されているプログラムのほか、利用者により作成されたプログラムも実行することができ、受信データの判別順序も利用者が定義できる。

【００４８】受信データの判別が出来たならば、データ検証手段２３にデータを供給する。判別が出来なければ、プログラム順序の次の（＝ＮＥＸＴ）プログラムにて受信データの判別を行う（ステップＣ１、Ｃ２、Ｃ３）。

【００４９】データ検証手段２３は、プログラム順序内でアクセス制御判別プログラムが格納されている場合には、プログラム順序に従い、データ検証方法補助記憶部２４に格納されたアクセス制御判別プログラムを実行する（ステップＤ１、Ｄ２）。

【００５０】プログラム順序内でアクセス制御判別プログラムが格納されていない場合には、データ検証方法記憶部３２から該当プログラムをデータ検証方法補助記憶部２４へ読み込み、プログラム順序に従い、データ検証方法補助記憶部２４に格納されたアクセス制御判別プログラムを実行する（ステップＤ２、Ｄ３）。

【００５１】但し、データ検証手段２３が始めて呼び出される場合には、データ検証方法補助記憶部２４にはアクセス制御判別プログラムは格納されていない。この場合には前述同様、データ検証方法記憶部３２から該当プログラムをデータ検証方法補助記憶部２４へ読み込み、プログラム順序に従い、データ検証方法補助記憶部２４に格納されたアクセス制御判別プログラムを実行する（ステップＤ２、Ｄ３）。

【００５２】データ検証手段２３はプログラム順序に従い、データ検証方法補助記憶部２４に格納されたアクセス制御判別プログラムを実行し、アクセスの可否を判断する。判別が出来なければ、プログラム順序の次の（＝ＮＥＸＴ）プログラムにてアクセス制御の判別を行う（ステップＤ１、Ｄ２、Ｄ３）。

【００５３】アクセス可否の判断結果が、アクセス不可ならば、データの受信を行わず、接続を切断する（ステップＤ３）。

【００５４】アクセス可否の判断結果が、アクセス可な

らば、プログラム順序にしたがって受信データ１件の取り込みを行う（ステップＣ１からＥまでを繰り返す）。

【００５５】受信データのすべての検証で接続可ならば出力装置４から、内部のネットワークへデータを送信し、ＮＥＸＴのデータ受信を待機する（ステップＦ、Ｇ）。

【００５６】上述の実施形態で実行されるプログラムは、予め標準製品として提供されているプログラムのほか、利用者により作成されたプログラムも実行することができ、アクセス可否の判別順序も利用者が定義できる。すなわち、記憶装置３に格納されているデータ検証順序記憶部３１と、データ検証方法記憶部３２とは、ファイアーウォール・プログラムとして市販されているプログラムを、図１には不図示のプログラムインストール装置によってインストールしたり、入力装置１を介してファイアーウォール用のフリーソフトウェアを入力してインストールして格納してもよく、また、利用者自体で作成した入力データの判別・検証用プログラムを格納してもよい。こうすることで、外部からの入力データに対するファイアーウォールとして、出力装置４に出力しても問題が生じないように、正当の可否判定・検証のため、柔軟性と拡張性を備えている。

【００５７】つぎに、図３に本ファイアーウォールシステムの動作処理のイメージ図を示す。先ず、公衆回線等の外部ネットワークからｅ－ｍａｉｌやデータ送受信の着呼があってデータが入力される。データ検証順序作成手段２２には、プログラム起動順序を指定している受信データ判別プログラムとデータ検証プログラムとが対となってデータ検証順序記憶部３１から、プログラムの実行順序に従って、起動順序の第１ではポート番号判定プログラムとポート番号検証プログラムを、第２では接続先判定プログラムと接続先判定プログラムとを読み込んでいる。また、データ検証方法補助記憶部２４は、ポート番号判定プログラムと、ポート番号検証プログラムと、接続先判定プログラムと、接続先判定プログラムとをプログラム起動順序に従って読み込んでいる。

【００５８】受信データ判別手段２１は、１回目プログラムが起動され、データ検証順序作成手段２２のプログラムに従って、先ずポート番号判定プログラムが実行され、入力データのポート番号がプログラムに則ったポート番号であるのかどうかを判定する。続いて、データ検証手段では、ポート番号検証プログラムに従って動作し、ポート番号の検証を行う。

【００５９】次に、２回目プログラムが起動され、データ検証順序作成手段２２の順序プログラムに従って、接続先判定プログラムが実行され、入力データの接続先がプログラムに則った接続先であるのかどうかを判定する。続いて、データ検証手段では、接続先検証プログラムに従って動作し、接続先の検証を行う。

【００６０】このように、本ファイアーウォールシステムでは、入力された受信データからポート番号と接続先の判定と検証を繰り返して、受信データが本ファイアーウォールにとって、正当か否かを判定・検証を行い、正当であれば、出力装置４に受信データを転送する。

【００６１】上記実施形態の動作の説明では、ポート番号と接続先によって判定・検証することを示したがこれに限られるものではなく、例えば、ＡＴＭ（非同期通信モード）では、ヘッダー部にネットワーキングのルートを示す指標が付してあるので、そのルートが正規であるのか否かを判定・検証材料としてもよく、またこれに類する判定・検証材料であってもよい。

【００６２】

【発明の効果】本発明によれば、第１に、アクセス制御のプログラムを追加出来ることにより、システムが提供していないデータ検証方法を、利用者が任意に作成可能なことである。

【００６３】この結果、ユーザがプログラムで自在に制御ルールを作成できるので、柔軟で高度なアクセス制御を実装することが可能になり、利用者がシステムの制限にとらわれることなく、データのアクセス制御を実現可能となる。

【００６４】また、第２に、プログラムを追加されることがはじめから念頭に置かれているので、プログラムの任意追加が出来るインタフェースを持つことにより、データ検証方法が新たに追加された場合、システムの再構築を行うことなく、新しい機能を使用可能とすることができる。

【図面の簡単な説明】

【図１】本発明による実施形態のファイアーウォールのシステム図である。

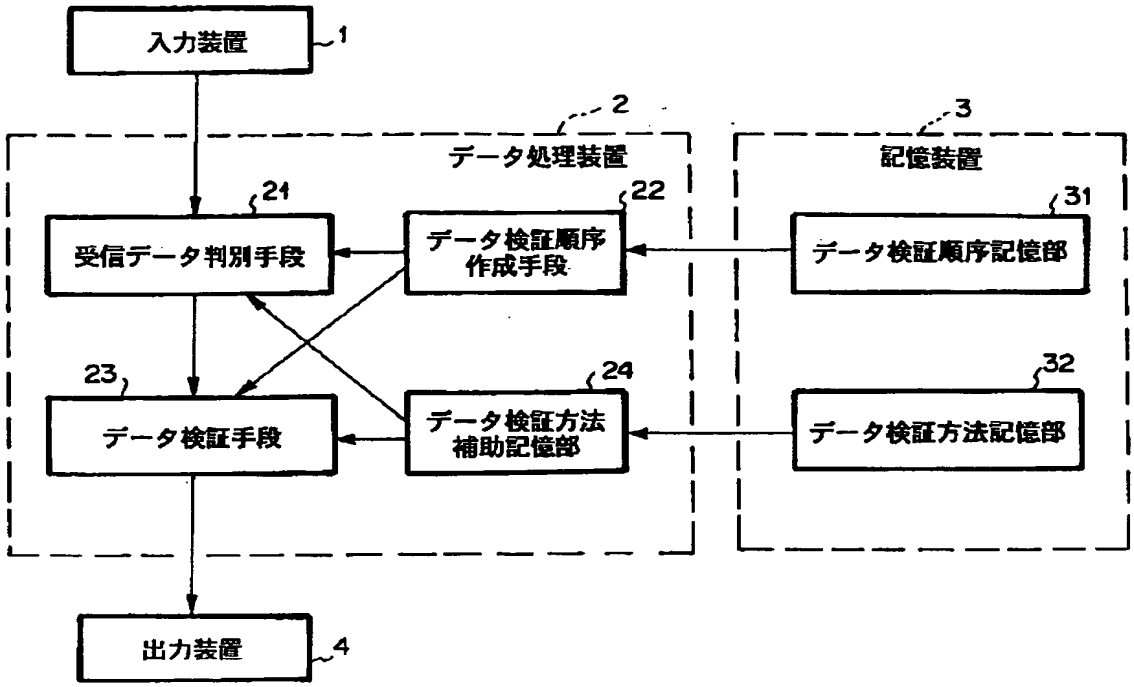
【図２】本発明による実施形態のファイアーウォールのフローチャートである。

【図３】本発明による実施形態のファイアーウォールの動作イメージ図である。

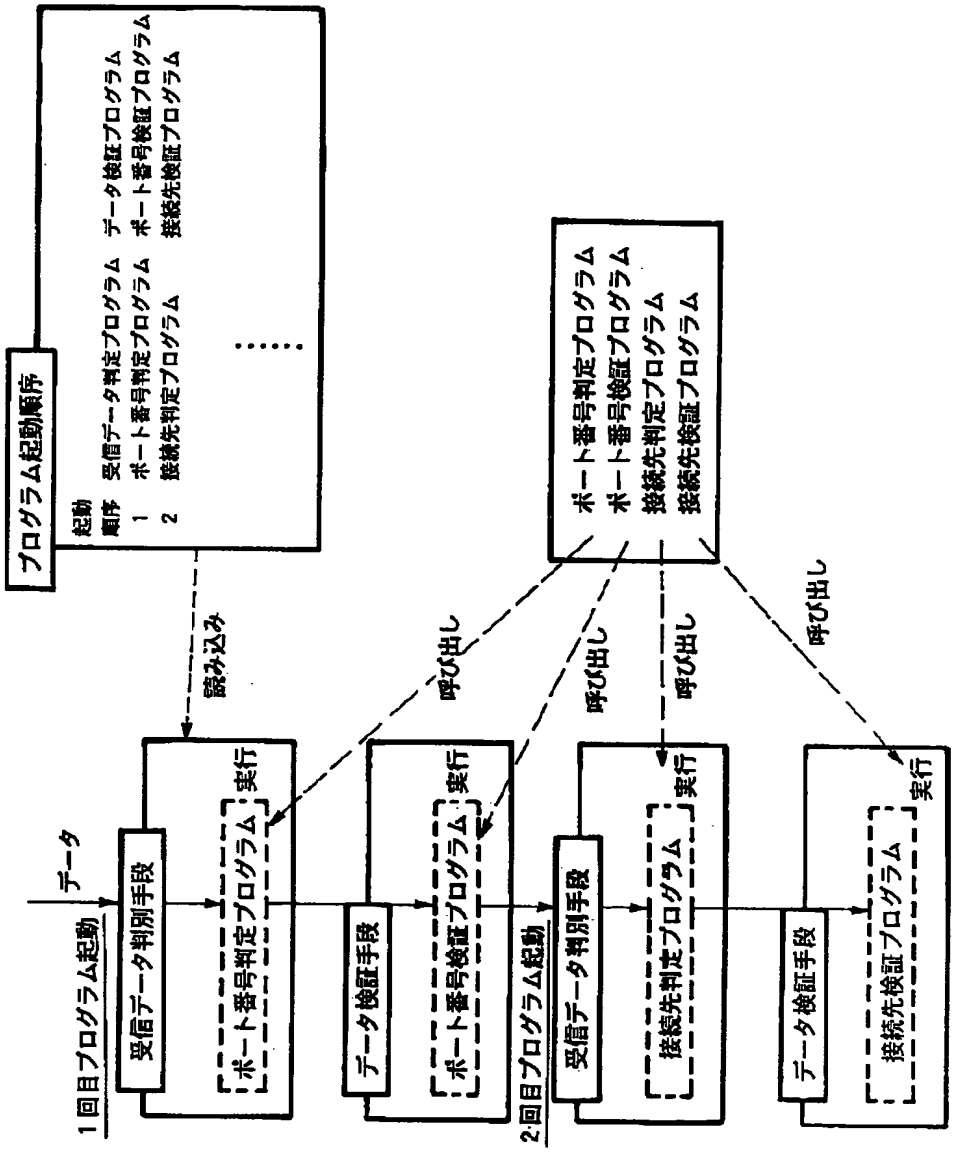
【符号の説明】

１　入力装置
２　記憶装置
３　データ処理装置
４　出力装置
２１　受信データ判別手段
２２　データ検証順序作成手段
２３　データ検証手段
２４　データ検証方法補助記憶部
３１　データ検証順序記憶部
３２　データ検証方法記憶部

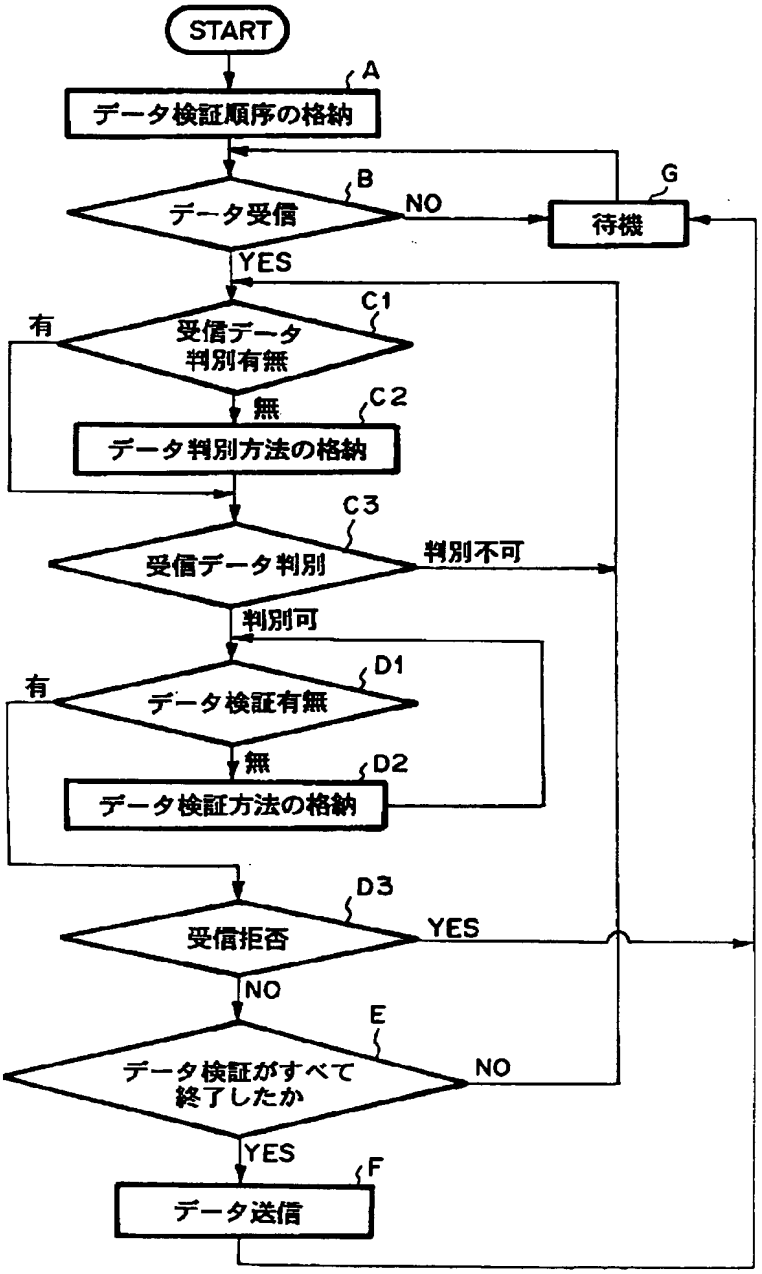
【図1】


入力装置
1
2
データ処理装置
3
記憶装置
21
受信データ判別手段
22
データ検証順序
作成手段
31
データ検証順序記憶部
23
データ検証手段
24
データ検証方法
補助記憶部
32
データ検証方法記憶部
出力装置
4

【図2】


プログラム起動順序
起動順序
1 受信データ判定プログラム
2 ポート番号判定プログラム
接続先判定プログラム
データ検証プログラム
ポート番号検証プログラム
接続先検証プログラム
読み込み
ポート番号判定プログラム
ポート番号検証プログラム
接続先判定プログラム
接続先検証プログラム
呼び出し
呼び出し
呼び出し
呼び出し
データ
1回目プログラム起動
受信データ判別手段
ポート番号判定プログラム 実行
データ検証手段
ポート番号検証プログラム 実行
2回目プログラム起動
受信データ判別手段
接続先判定プログラム 実行
データ検証手段
接続先検証プログラム 実行

【図3】


START
A
データ検証順序の格納
B
データ受信
NO
G
待機
YES
C1
受信データ判別有無
有
無
C2
データ判別方法の格納
C3
受信データ判別
判別不可
判別可
D1
データ検証有無
有
無
D2
データ検証方法の格納
D3
受信拒否
YES
NO
E
データ検証がすべて終了したか
NO
YES
F
データ送信